

IN THE CLAIMS

1. (Currently amended) A method for preventing receipt by receivers of unwanted electronic mail messages (email) sent by senders in a communication system, comprising the steps of:

determining whether email to a particular receiver comprises valid message authentication code (MAC) information;

filtering out at a gateway of the communication system email directed to the particular receiver that does not comprise valid MAC information; ~~and~~

providing the particular receiver with email directed to the particular receiver that comprises valid MAC information;

determining if a particular sender is a registered sender of email to the particular receiver, wherein the particular sender becomes a registered sender by satisfying a requirement; and

registering the particular sender when the particular sender is determined not to be a registered sender of email to the particular receiver;

wherein the step of registering the particular sender comprises the steps of:

establishing by the particular sender a cookie which indicates to the particular receiver whether the particular sender has satisfied the requirement to allow the particular sender to become a registered sender to the particular receiver;

establishing an address related to an address associated with the particular receiver which will inform the particular sender that the particular receiver desires that the particular sender be able to send email to the particular receiver; and

establishing by the particular receiver a key which is forwarded to the particular sender by the particular receiver to inform the particular sender that the particular sender is authorized to send email to the particular receiver and is now a registered sender and for use by the particular sender whenever the particular sender wishes to send email to the particular receiver;

wherein said step of establishing the address comprises generating a pseudorandom function with a keyed hash function using an input number comprising a unique serial number for use in generating an identifier for email between the particular sender to the particular receiver.

2. (Canceled)

3. (Canceled)

4. (Currently amended) The method recited in claim [[2]] 1, wherein said step of establishing an address comprises sending email from the particular receiver to the particular sender using public key encryption.

5. (Currently amended) The method recited in claim [[2]] 1, wherein said registering step further comprises sending to the particular user by the particular receiver, an encrypted key wherein the encrypted key is a member of a set of encrypted keys.

6. (Original) The method recited in claim 5, further comprising the step of storing the encrypted key by the particular sender in a table of encrypted keys for use by the particular sender whenever the particular sender desires to send email to the particular receiver.

7. (Canceled)

8. (Previously presented) The method of claim 1, wherein the step of determining whether email comprises valid MAC information comprises comparing the MAC against a value determined by the particular receiver.

9. (Previously presented) The method recited in claim 1, wherein the step of determining whether email comprises valid MAC information comprises comparing the MAC to an available header in an address of the particular receiver, in the received email message, whereby the MAC is not a valid MAC if the MAC and the header are not identical.

10. (Currently amended) A server for preventing receipt by receivers of unwanted electronic mail messages (email) sent by senders in a communication system, comprising:

a determining module for determining whether email to a particular receiver comprises valid message authentication code (MAC) information[[]];

a filtering module for filtering out at a gateway of the communication system email directed to the particular receiver that does not comprise valid MAC information[[]]; and

a provisioning module for providing the particular receiver with email directed to the particular receiver that comprises valid MAC information; and

a registering module for determining if a particular sender is a registered sender of email to the particular receiver, wherein the particular sender becomes a registered sender by satisfying a requirement;

wherein the registering module is also for registering the particular sender when the particular sender is determined not to be a registered sender of email to the particular receiver; and

wherein said registering module further comprises a generator for generating a pseudorandom function with a keyed hash function using an input number comprising a unique serial number for use in generating an identifier for email between the particular sender to the particular receiver.

11. (Canceled)

12. (Currently amended) The server recited in claim [[11]] 10, wherein said registering module sets up an encrypted address for sending email from the particular receiver to the particular sender using public key encryption.

13. (Currently amended) The server recited in claim [[11]] 10, wherein said registering module sends to the particular user by the particular receiver, an encrypted key wherein the encrypted key is a member of a set of encrypted keys.

14. (Canceled)

15. (Previously presented) The server of claim 10, wherein said filtering module compares the MAC against a value.

16. (Previously presented) The server recited in claim 15, wherein the filtering module compares the MAC to an available header in an address of the particular receiver, in the received email message, whereby the MAC is not a valid MAC if the MAC and the header are not identical.

17-20. (Canceled)